הפחדה מכוונת או בעיה אמיתית?

מומחי סייבר מתריעים מפני תרחיש 'יום הדין' – פגיעה בתשתית קריטית של מדינה שתגרום להרג של אלפי אנשים באמצעות תקיפת סייבר

מאת דניאל ארנרייך

חמ"ל תחנת חשמל (Bigstock :צילום)

ערכות בקרה (Industrial Control Systems (ICS מפקחות על ייצור אנרגיה, מים וביוב, דלק וגז, מפעלים תעשייתיים, מתקנים ביטחוניים ותשתיות קריטיות אחרות. מרבית הסוגים של מרכזי הבקרה כגון SCADA, DMS, BEMS, DCS ו- EMS הותאמו בעיקר לפעול באמינות גבוהה, והנושא של אבטחה קיברנטית (Cyber Security) לא נכלל כדרישה חשובה. לעוסקים בתפעול ובתחזוקה ידוע כי גיל מערכות אלה נע בין 15–7 שנים, וזו עוד סיבה להימנע משאננות. ידוע כי המשאבים שעומדים לרשות התוקפים ממומנים על ידי מדינות עוינות, גופים מסחריים וארגוני פשע, ולכן ההגנה על מתקנים קריטיים הפכה לאתגר משמעותי. בהתייחס למגמות אלה, השאלה היא לא האם אירוע חמור ברמה של פגיעה לאומית (כמו 11–9) עלול להתרחש, אלא כיצד להבטיח את המשכיות התפעול (Business continuity) של מתקנים קריטיים אחרי אירוע מסוג זה.

האם האיום אמיתי?

בנושא זה הדעות חלוקות. תלוי במומחה ובמסגרת איזה כנס הוא מדבר, ובאיזה יום הוא שם כובע של "מרגיע לאומי" או כובע של "נביא הזעם". במערכות IT, יש ההקפדה על סודיות, זמינות ואמינות נתונים (CIA-Confidentiality, Integrity, Availability), אבל במערכות בקרה הדגש העיקרי הוא על תפעול בטוח ואמין (Safety and Reliability). נושא הסודיות נדחק לתחתית, מכיוון שבמערכות התפעול לא נדרש להסתיר את הערכים (פרט למקרים חריגים) המעוברים בין מגוון הבקרים במערכת לבין מרכז הבקרה.

בהתייחס לתשתיות קריטיות, אין לאף מנהל סמכות להרגיע באופן גורף וגם לא לנבא את ה"אסון שבדרך", וכל יום צריכים לצפות לאיומים חדשים מסוג שעדיין לא ראינו. על עובדה אחת אין מחלוקת, שבכל מערכות מחשוב יש תקלות תוכנה (Bugs) שגורמות לחולשה באבטחה (Security Vulnerability), ובגלל קיומן של אלה נשקפות סכנות ממשיות לתשתיות קריטיות. חולשות אלה חושפות את מערכות הבקרה לתקיפות זדוניות שהוחדרו בדרך כלשהי ואת כוחם לגרום לנזקים.

להלן מספר דוגמאות: התקפות מסוגDoS – Denial of Service או החמור יותר Distributed Denial of Service – DDoS שמטרתם לבצע השבתה של תפקוד מערכת הבקרה, אך ללא גרימת נזק למתקן. שליטה מרחוק מפעילה "סוכן פנימי" Remote Administration Trojan RAT לתקיפה המאפשרת השתלטות והרצה של תוכנות זדוניות במטרה לגנוב מידע, לרגל אחרי תהליכים וליצור שם משתמש וסיסמה עבור מתחזה. מטרתם של תקיפות מסוג Man in the Middle – MitM היא לשבש את תפקוד הבקרה באמצעות שיבוש ערכים תפעוליים, דיווח על ערכים מזויפים, יצירת נזקים כספיים ונזק למתקן, דומה למה שקרה באירוע Stuxnet.

הרשויות לאבטחת מידע והגנה קיברנטית שואפות למזער את הסיכונים על ידי הפחתה מראש של מספר נקודות החולשה, ולזהות מהר ככל שניתן את מסלולי התקיפה. הכשלים במערכות משתייכים למספר קטגוריות, ויש להתייחס לאלה במלוא כובד הראש. אבטחה פיזית לא נאותה: ידוע כי לא ניתן להפעיל אבטחה קיברנטית אמינה ללא הגנה פיזית יעילה שתמנע מגורם לא מורשה לחדור לאזור מאובטח ESP (electronic security perimeter).

חשיפה לתחילת התקיפה דרך דוא"ל. קיימת חוסר מודעות בכל הקשור לפניות "ידידותיות" דרך דוא"ל. פתיחת מכתב כזה עלולה לגרום להתקנה של מקליט את המקלדת (keystroke logger) במטרה לשדר נתונים לגורם עוין. הזנחה לגבי שדרוג החומרה. ציוד מיושן לא חסין בפני תקיפה קיברנטית ומצב זה עלול לערער את חוסן המערכת (system resiliency). הסיבות המוצדקות לבעיה זו גרמו ל "חוסר מדיניות" בנושא שדרוגים.

ניהול סיסמאות רשלני. קיים קושי לתקן מנהגים של אנשים בכל הקשור לאבטחת קיברנטית. לעתים אנו נתקלים באנשים שהם חסרי אמונה לסכנות שנובעות מסיכוני תקיפה. שימוש באנטי-וירוס לא עדכני. עדכונים מבוצעים לעתים רחוקות בלבד בשל החשש לשיבוש הפעולה של מערכת הבקרה, ואי הודאות (מוצדקת) לגבי תפקוד האנטי-וירוס עם מערכות בקרה. ארכיטקטורת רשת לא תקינה: מערכות עם יחידות IED, PLC ,RTU מיושנות שתוכננו לפני שנים בנויות באופן "שטוח" ללא הפרדה נאותה בין אזורים לצורך חסימת מעברים לא מורשים (Security Zoning).

חיבור לרשת אינטרנט. אנשים סבורים בשוגג שאם מערכות הבקרה מקושרות לאינטרנט באופן עקיף (דרך הרשת הארגוניתCorporate Network) ורכיב חומת אש (FW), הם בטוחות בפני תקיפה קיברנטית. התפשטות קוד מזהם (malware), ללא הפרדה בין אזורים, תקיפה פנימי על ידי התקן USB או דומה (internal attack), או חיבור אלחוטי לתחזוקה (Backdoor) יאפשרו התפשטות של קוד המזהם במערכת.

תצורה של מערכת הפעלה. מחשבי הבקרה חייבים לפעול ברציפות ללא אפשרות ביצוע עדכוני תוכנה (Software Patching), ובמערכות רבות לא מבצעים הקשחה (Hardening) וחסימת חיבורים (Ports) לא חיוניים. תצורה של מערכות הגנה. תכנות של חומת אש (firewall provisioning) הוא תהליך מורכב ככל שהמוצר מתוחכם יותר. תכנות פגום או תקיפה על ידי אתחול הרכיב (Reset attack), עלולים להפוך אותו ל"שקוף".

צילום: Bigstock

> "הרשויות לאבטחת מידע והגנה קיברנטית שואפות למזער את הסיכונים על ידי הפחתה מראש של מספר נקודות החולשה, ולזהות מהר ככל שניתן את מסלולי התקיפה"

כיצד ניתן להתגונן?

נקודות התורפה שצוינו לעיל הן רק חלק קטן מרשימה ארוכה של מסלולי תקיפה על תשתיות קריטיות, וההגנה עליהם אינו אתגר פשוט (Critical Infrastructure Protection – CIP), בעיקר בשל מורכבות המערכות. הואיל ואין פתרון יחיד ובר השגה לכלל האיומים (there is no silver bullet), התהליך למזעור הסיכונים של תקיפה קיברנטית (cyber risk mitigation) נעשה באמצעות "טיפול מונע" במספר רמות.

השימוש במערכות חומת אש (Firewall) ומערכות אזור מפורז (Demilitarized Zone) נועדו לסננן מעבר מידע לא מורשה. רכיבים אלה מותקנים מאז הקמת המערכת וחייבים לשדרג אותם בהתמדה. פתרונות אבטחה שמתמקדים בבחינת שלמות המידע (data integrity)

Bigstock :צילום

נותנים הגנה נוספת בפני התקיפות קיברנטיות יישום פתרונות הגנה מסוג Intrusion Detection System – IDS וגם Intrusion Prevention System – IPS פועלים באמצעות ניתוח המידע שנאסף ממספר נקודות ברשת באמצעות חיישנים (data sniffers, taps). IDS מאפשר דיווח למרכז השליטה Security Operation Center–SOC ו IPS מבצע חסימת גישה.

מגוון סוגי "חומת אש" עבור מערכות בקרה (SCADA-aware Firewall) מבצעים בחינה על ה"תוכן" (payload) שבתוך המידע ומסוגלים לאתר אם בוצעה שינוי כלשהו (Data Integrity). באמצעות תהליכים מעמיקים (Deep Packet Inspection) ניתן לאתר תקיפות מסוג MitM. חשוב לציין כי אין להשתמש בהצפנה "פרטית" אלא רק בתהליך סטנדרטי מבוסס על AES 256 (Kerckhoffs's principle). השימוש באמצעי הצפנה (למרות שלא תמיד נדרש) מקשה על תקיפות מסוג MitM כיוון שאין ביכולתם לשנות ערכים ויסתפקו רק בשידור חוזר של המסר (message replay) בצורה עיוורת.

תקיפות מסוג "יום אפס" (Zero day attack) מנצלות חולשות במערכת שנודע לגביהם באותו יום (Zero day vulnerability) ועדיין לא קיימים אמצעי הגנה. פתרונות תוכנה המבצעים זיהוי התנהגות חריגה מבחינה של תקשורת או תהליכי הבקרה (Anomaly detection) יפעלו באופן יעיל לאיתור תקיפות אלה.

סריקות מחזוריות של המערכת (periodic scanning) לגבי בקרים מותקנים, גרסאות תוכנה, רמת הזיכרון הפנוי, יכולים לשמש כתהליך "לימוד עצמי" (self-study). תהליך זה מאפשר לגלות פעילות חריגה מכל סוג, כלל לגבי פעולות של אנשים מורשים (authorized personnel) לבצע תחזוקה במערכת.

פתרונות למעבר מידע "חד-כיווני" Unidirectional Security Gateway (ידוע גם בשם Diode) נועדו לבצע הפרדה בין אזורים. התנאי למימוש אפשרי בפתרון זה הוא, כי המידע יזרום רק בכיוון אחד, בדרך כלל החוצה מהאזור מערכת הבקרה, ואין שום דרך להעברת נתונים בכיוון ההפוך – לתוך המערכת.

הגנה מערכתית Security Information Event Monitoring – SIEM מתמקדת באבחון התקיפה באמצעות ניתוח המידע ממספר מוקדים. זיהוי התקיפה בתהליך זה מתבצע על ידי "הצלבת-מידע" המסופק למערכת SIEM. חשוב להדגיש כי המידע מעובר באופן חד-כיווני על מנת למנוע סיכוני תקיפה על המערכת.

צו השעה – הקצאת משאבים

מספר וחומרת התקיפות הולכות וגוברות כי היום התוקפים הממומנים מכספי מדינות עוינות, ארגוני פשע וארגונים מסחריים ופועלים לגרימת השבתה, נזק או יצירת רווחים. למרות שאין מידע מוקדם לגבי המועד לאירוע תקיפה, הסיכון וגם הסיכוי לתקיפה קיברנטית גוברים. המסקנה המתבקשת היא, שמפעילים של מתקנים קריטיים חייבים לפעול ביתר נחישות וחוכמה כדי להיות "צעד אחד לפני התוקפים". תובנה זו חייבת להוביל להשקעה משמעותית והקצאת ומשאבים מכיוון שפגיעה בכל אחת מהתשתיות מהווה איום חמור על הביטחון ורווחת אזרחי המדינה.

דניאל ארנרייך (BSc). הוא יועץ עצמאי במסגרת מומחים לבקרה ותקשורת מאובטחת (SCCE) בעל ניסיון של מעל 25 שנים בנושא מערכות בקרה על תשתיות קריטיות כגון: חשמל, מים, גז, ומערכות בקרה על תחנות כוח במסגרת פעילותו בחברות מוטורולה, סימנס ווטרפול סקיוריטי